Continuation of Application for Search Warrant

I, Heather Williamson, being duly sworn, state as follows:

I. Introduction

1. I make this continuation of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – cellular telephones, as described in Attachment A – that are currently in the possession of law enforcement, and the extraction of electronically stored information from that property as described in Attachment B.

2. I am a Special Agent of the Drug Enforcement Administration ("DEA") and have been so employed since January 2013. I am currently assigned to the Grand Rapids District Office. Previously, I was assigned to the Southwest Border Initiative Group-3 ("SWB-3") and to the Los Angeles Strike Force for approximately six years. The Los Angeles Strike Force is an investigative group jointly led by the DEA and the FBI, and composed of several other federal, state, and local agencies that is focused on the disruption of the Mexico-based Sinaloa Cartel. Prior to working as a DEA Special Agent, I completed 20 weeks of training at the DEA Academy in Quantico, Virginia, which included instruction in narcotics identification, detection, trafficking, and interdiction; money laundering techniques; asset identification, seizure, and forfeiture; and techniques used by narcotics traffickers to avoid detection by law enforcement officials. I have investigated drug trafficking organizations involved in violating various federal laws, including, but not limited to, unlawful importation of controlled substances; the distribution of

controlled substances; manufacturing of controlled substances; and possession with intent to distribute controlled substances, including cocaine, methamphetamine, heroin, and other dangerous drugs; as well as money laundering. I have participated in investigations of unlawful drug trafficking and money laundering and, among other things, have conducted or participated in surveillance; execution of search warrants; debriefings of informants; reviewing of taped conversations and drug records; and have participated in investigations that include the interception of wire communications.

3. Through my training, education and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the methods of payment for such drugs, the laundering of narcotics proceeds, and the dialect (lingo) and coded language used by narcotics traffickers. In connection with my duties, I investigate criminal violations of the federal and state controlled substance laws, including, but not limited to, conspiracy and attempt to possess with intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); use of communication facilities to facilitate drug trafficking offenses, in violation of Title 21, United States Code, Section 843(b); and offenses involving money laundering as well as conspiracy and attempt to do the same, in violation of 18 U.S.C. §§ 1956 and 1957. Many of these investigations also involve firearms offenses, including violations of 18 U.S.C. §§ 922(g) and 924(c).

4. Because this Continuation is for the limited purpose of establishing probable cause to support the issuance of search warrants against the proposed subject device, it contains only a summary of relevant facts. I have not included each and every fact known to me or to other law enforcement officers concerning the entities, individuals, and events described in this Continuation.

5. The statements contained in this Continuation are based in part on: (a) my personal participation in this investigation; (b) information provided by other federal law enforcement officers, West Michigan Enforcement Team (WEMET); (c) laboratory analysis reports; (d) surveillance reports; (e) criminal history records; (f) information from confidential informants; and (g) my training and experience and the training and experience of other law enforcement agents.

I. Overview of Investigation

6. This Continuation is based on the Drug Enforcement Administration's (DEA) and WEMET's investigation into the drug trafficking activities of Alezay COLEMAN and his criminal associates. On January 29, 2021, Magistrate Judge Phillip J. Green of the United States District Court for the Western District of Michigan issued an arrest warrant pursuant to a criminal complaint charging COLEMAN with possession with intent to distribute 50 grams or more of methamphetamine, a Schedule II controlled substance, and a mixture or substance containing a detectable amount of heroin, a Schedule I controlled substance, and N-phenyl-N-[1-(2-phenylethyl)-4-piperidinyl] propanamide (fentanyl), a Schedule II controlled substance, in violation of 21 U.S.C. § 841(a)(1), (b)(1)(A)(viii), (b)(1)(C).

See United States v. Coleman, No. 21-MJ-00037. The facts stated in that continuation are incorporated by reference herein.

7. On February 2, 2021, the United States Marshals and other investigators executed the arrest warrant of COLEMAN. COLEMAN and two other individuals were observed entering a residence in Muskegon, Michigan. At approximately 12:45 PM, COLEMAN exited that residence alone carrying a backpack, at which point investigators moved in, notified COLEMAN that he was under arrest, and detained him.

8. In the backpack, investigators found approximately 113.65 grams of fentanyl, 49.4 grams of methamphetamine, 14.92 grams of cocaine, 13.31 grams of heroin, and a digital scale.[1] Investigators also found:

a. One black Apple iPhone 11 located on COLEMAN's person on February 2, 2021 (**Subject Device 1**)

b. One black ZTE flip phone located on COLEMAN's person on February 2, 2021 (**Subject Device 2**)

c. On pink Apple iPhone 6S located on COLEMAN's person on February 2, 2021 (**Subject Device 3**, collectively referred to with **Subject Device 1** and **Subject Device 2** as the **Subject Devices**.)

9. The **Subject Devices** are in the custody of the Michigan State Police Computer Crimes Unit.

[1] All weights are approximate weights and the drug analysis is based on field testing using a TrueNarc device. Further laboratory testing is pending.

II. PROBABLE CAUSE

A. COLEMAN'S Historical Use of Cell Phones to Communicate about Drug Trafficking

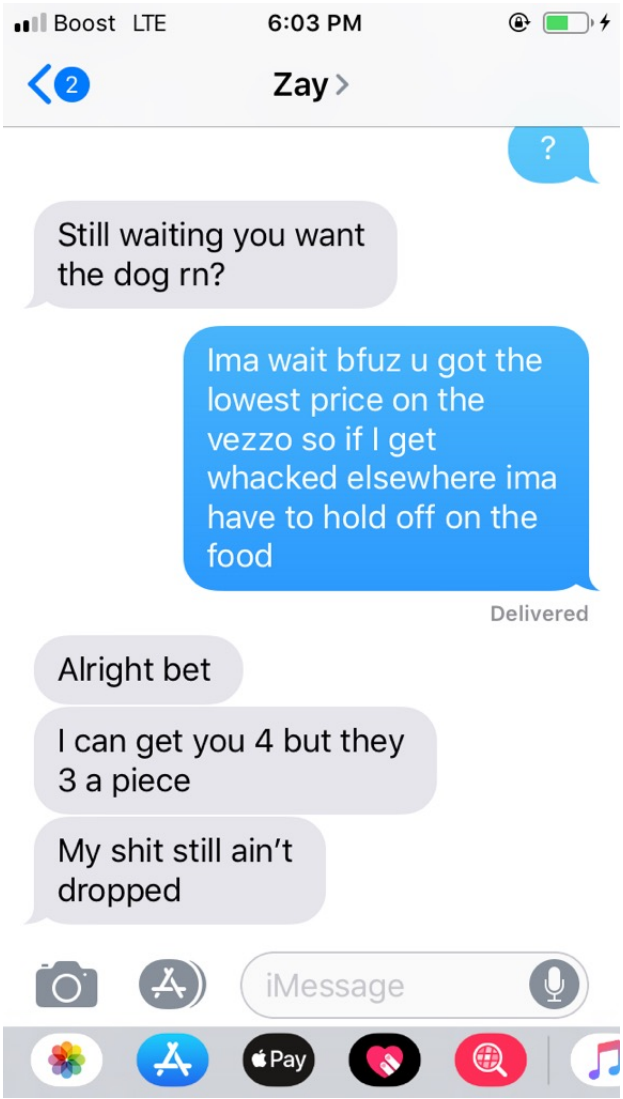
10. Based on my training, experience, and familiarity with the investigation, I know that drug traffickers use their phones to communicate about drug trafficking. Specifically, I know that COLEMAN texts about drug trafficking. For example, COLEMAN had a number of communications with a confidential informant discussing drug trafficking. On November 14, 2019, in the presence of an investigator, CS-1 contacted COLEMAN at phone number (323) 326-0029, which is believed to be **Subject Device 1**, to coordinate the purchase of 3 grams of heroin for $225 from COLEMAN's residence, 935 Ada Avenue, Muskegon, Michigan.[2] As outlined in the continuation in support of the criminal complaint in more detail, the controlled buy was successfully completed from COLEMAN.

11. On November 18, 2019, in the presence of investigators, CS-1 contacted COLEMAN at phone number (323) 326-0029, believed to be **Subject Device 1**, to coordinate the purchase of three ounces of crystal methamphetamine for $900 at 935 Ada Avenue. As outlined in the continuation in support of the criminal complaint in

[2] On December 9, 2019, investigators executed a federal search warrant at COLEMAN's residence at 935 Ada Avenue in Muskegon, Michigan. Investigators detained COLEMAN, and found on his person a black iPhone with the phone number (323) 326-0029, which is the same make and color as **Subject Device 1**. From phone toll information and Cellebrite downloads of defendants in other cases, I know that COLEMAN has continued to use the phone number (323) 326-0029 throughout 2020.

more detail, the controlled purchase of 87 grams of crystal methamphetamine was successfully completed.

12. On December 2, 2019, in the presence of investigators, CS-1 contacted COLEMAN at phone number (323) 326-0029, believed to be **Subject Device 1**, to coordinate the purchase of two ounces of crystal methamphetamine for $600 at 935 Ada Avenue. Below is a screen grab of text messages between COLEMAN and CS-1:



Based on my training, experience, and familiarity with the investigation, I know the word "vezzo" to be a code word used by drug traffickers in the Western District of

Michigan for methamphetamine. I also know that "food" is a common reference to heroin. When COLEMAN said "I can get you 4 but they 3 a piece," I believe he meant that he could get up to four ounces of methamphetamine for $300 an ounce. As outlined in the continuation in support of the criminal complaint in more detail, the controlled buy was successfully completed from COLEMAN.

13. Based on evidence in the investigation, I know that COLEMAN has continued to distribute narcotics in 2020 and up to the date of his arrest. Most significantly, on February 2, 2021, COLEMAN was arrested and possessed a backpack containing 113.65 grams of fentanyl, 49.4 grams of methamphetamine, 14.92 grams of cocaine, 13.31 grams of heroin, and a digital scale. Based on my training and experience, I know these quantities to be distribution quantities. I also know that digital scales are common tools of the drug trafficking trade used to weigh individual quantities of narcotics for distribution. COLEMAN also possessed the **Subject Devices** on his person.

14. I know from training and experience that drug traffickers frequently utilize mobile telephones to facilitate drug transactions. I also know that drug traffickers often keep multiple phones. For example, a drug trafficker may have one phone that he uses to communicate with his suppliers and a separate phone that he uses to communicate with his customers.

15. Drug traffickers rely upon voice phone services, SMS and MMS text messaging, social media instant messaging services, and electronic mail apps to communicate with suppliers, customers, and confederates. Mobile telephones are

portable and phone providers often do not require purchasers or users of the devices to provide their true names and/or addresses, so drug traffickers often maintain multiple devices to avoid detection by law enforcement. Mobile phones often contain evidence indicative of drug trafficking, including records of incoming and outgoing calls; text messages; photographs of narcotics, coconspirators, or currency; and, in the case of "smart phones," Global Positioning System ("GPS") data indicating the location of the device at given points in time.

16. Based on my training and experience, I know that electronic devices such as the **Subject Devices**, can be used to store electronic information for long periods of times, including years. Even if a drug trafficker is being cautious of law enforcement detection and deleting the substance of communications, significant data may still remain on the phone, such as call logs, contact information, photographs, wireless internet connections (which can reveal location information), and other location information.

17. Further, based upon my training, experience, and participation in drug investigations and financial investigations relating to drug investigations, I am aware of the following:

a. Drug traffickers often keep names, aliases, and/or contact information of suppliers, purchasers, and others involved in drug trafficking in their devices;

b. Drug traffickers sometimes use electronic messaging or messaging apps, in addition to MMS, SMS text messages, and

voice call, to communicate with suppliers, purchasers, and others involved in drug trafficking on their devices;

c. Drug traffickers often take pictures or videos of their drug trafficking associates, drugs, money and/or firearms, which they store on their devices;

d. That drug traffickers often maintain, on hand, large amounts of currency in order to maintain and finance their on-going narcotics business and often store information related to the profits of their narcotics trafficking on their devices;

e. Global Position System (GPS) data on phones may show the location of a drug trafficker at a given time, which may provide corroborating evidence of a drug delivery or other instance of drug trafficking;

f. User attribution data and usernames, passwords, documents, and browsing history can provide evidence that the device is being used by a drug trafficker and can provide other useful evidence to the drug investigation;

g. Drug traffickers often use the Internet to look up various information to support their drug trafficking activities on their devices;

h. That drug traffickers often have unexplained wealth and assets as they do not have a job, nor do they report income on their

state or federal tax returns. Subjects often use cash, money orders, and cashier's checks, and prepaid debit cards as a way of purchasing items as a way to disguise where the funds are ultimately coming from. Subjects will place assets in the names of nominees, which are often friends and family members in an attempt to hide the true ownership of the assets. It is common for drug traffickers to maintain books, records, receipts, notes, ledgers, receipts relating to the purchase of financial instruments and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them, including their devices;

i. That it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and or expenditure of drug proceeds on their devices. This evidence includes information related to currency, financial instruments, precious metals and gemstones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts,

cashier's checks, bank checks, safe deposit box receipts or keys, records concerning storage lockers and money wrappers; and

j. That drug traffickers frequently receive their supply of drugs through packages sent by U.S. Mail or third-party delivery service and frequently keep copies of tracking numbers, receipts and photographs of packaged narcotics on their devices.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen

for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global

positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training and experience, I believe that the **Subject Device** has capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that

might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Devices** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Devices** because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

B. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

C. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire

medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant sought in this continuation seeks only permission to examine devices should they come into law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant for search of the **Subject Devices** at any time in the day or night.

III. Conclusion

24. Based on the above information, I believe that there is probable cause to search the **Subject Devices**.